6-2020

From Degree to Chief Information Security Officer (CISO): A Framework for Consideration

Wendi M. Kappers
Embry-Riddle Aeronautical University, kappersw@erau.edu

Martha Nanette Harrell,
Arkansas Tech University

From degree to Chief Information Security Officer (CISO): A framework for consideration.

Dr. Wendi M. Kappers, Embry-Riddle Aeronautical University - Daytona Beach

Wendi M. Kappers has a Ph.D. in Instructional Technology from the University of Central Florida (UCF). Her thesis work explored how educational video game effects upon mathematics achievement and motivation scores differed between the sexes. During her tenure at Seminole Community College working as a tenured Professor and Program Manager of the Network Engineering Program, she was Co-PI for the CSEMS NSF grant that explored collaborative administration and industry mentorship planning used to increase enrollments of woman and minorities with declared majors in the areas of Computer Science (CS), Engineering (E), Mathematics (M), and Science (S). Currently, Dr. Kappers is an Assistant Professor within the M.S. in Information Security & Assurance (MISA) within Embry-Riddle Aeronautical University's (ERAU) College of Business, Worldwide Campus, and teaches within the College of Engineering for the Daytona Beach Campus of ERAU. Teaching responsibilities include: RSCH 202 – Introduction to Research, CS120 – Introduction to Computing in Aviation, and the entire collection of MISA-related program courses as needed. Both positions allow her to stay focused upon real-life educational and classroom issues while designing courses that explore technology utilization that is based on structured learning principles and practices. She is an experienced Computer Engineer, Teaching and Learning Center Director, and an Instructional Designer, designing in Blackboard, WebCT, eCollege, and Canvas, and holds many industry-related certifications including the Microsoft Certified Systems Engineer (MCSE) and Trainer (MCT) certificates.

Dr. Martha Nanette Harrell, Arkansas Tech University

Dr. Nan Harrell is an assistant professor in the College of Engineering and Applied Science for Arkansas Tech University. Prior to this position, she was the Information Systems Manager and Cyber Security Officer for the Arkansas Office of Health Information Technology (OHIT). She worked with the team at OHIT to implement the State Health Alliance for Records Exchange (SHARE). Dr. Harrell has over 25 years' experience with the technology field, serving as an educator, implementer, and manager. Dr. Harrell is a certified Project Manager and a Certified Public Manager. She has worked with the Arkansas State Cyber Security Office to ensure successful implementation of many State security projects, one of which received the George C. Askew Outstanding Project Award for Certified Public Managers.

From degree to Chief Information Security Officer (CISO): A framework for consideration

Abstract: Educational entities are establishing program degree content designed to ensure cybersecurity and information security assurance skills are adequate and efficient for preparing students to be successful in this very important field. Many Master's level programs include courses that address these skills in an attempt to provide a well-rounded program of study. However, undergraduates who are in the practitioner's world have other alternatives to gain these skills. These individuals can gain various certifications, such as the Certified Information Systems Security Professional (CISSP) or the Certified Information Security Manager (CISM). Due to a perceived gap between academics and field knowledge, it appears that academic programs may not fully consider the very specific competencies of C-Suite members (e.g. Chief Information Security Officer (CISO)) since field certification may be the only validation of such skills. Therefore, a framework from degree to industry employment acceptance is needed.

To this end, the current study suggests the use of a framework in which to examine and compare C-Suite competencies versus academic preparations. Ultimately, this framework will assist researchers in examining the actual, current job tasks of C-Suite members. Since the CISO position is new to the industry, becoming a common job title within only the last few years, the reporting structure for the CISO varies widely and various organizations have differing expectations of the position [1]. Therefore, the initial phases of this study focus solely upon this position as the starting benchmark.

This paper explores historical aspects of the workforce skills gap in the area of computer security while providing survey validation results from Phase I of this project. This pilot investigation invited faculty (n=5; 24% response rate) who are both practitioners and academicians to support this examination and the acceptance of said framework. Demographic data includes a comparison between degree attainment and employment position, and asked respondents to compare academic preparatory tasks to that of required job market skills - those skills collected from the literature and employment position descriptions taken from Yahoo, Google, Monster, Indeed, and other HR-advertised locations.

Lastly, respondents were asked to rank these skills by importance to establish the framework baseline of comparison. Future phases of this project will include a larger sample and Delphi results gathered during the ranking phase of this effort. Recommendations for future program designs will be provided upon the completion of the overall study.

Keywords: C-Suite, Skills gap, CISO, Security, Information Assurance, Curriculum, Industry Competencies

I. Introduction

Educational entities are establishing program degree content designed to ensure cybersecurity and information security assurance skills are adequate and efficient for preparing students to be successful in this very important field. However, the higher-level career position, such as the CISO, is fairly new and requires extensive knowledge and skills to ensure success. Many Master's level programs include courses that address these skills in an attempt to provide a well-rounded program of study, but undergraduates who are in the practitioner's world have other alternatives to gain these skills. These individuals can gain various certifications, such as the

Certified Information Systems Security Professional (CISSP) or the Certified Information Security Manager (CISM). Due to a perceived gap between academics and field knowledge, it appears that academic programs may not fully consider the very specific competencies of C-Suite members (e.g. Chief Information Security Officer (CISO)) since field certification may be the only validation of such skills. Therefore, this work-in-process seeks to investigate the use of a framework to examine the degree to industry employment skill variance, if any, between industry and academic preparation and the perceived required skills that each group expects the graduate to have mastered.

Previous research used a systematic approach, such as DACUM, to integrate the perceptions of practitioners in the field with that of the academicians to establish the desired curriculum. This process is especially useful when the degree is designed to meet emerging new occupations or job titles, such as the Chief Information Security Officer [2][3]. However, little research can be found that uses the establishment of a skill set for the C-Suite level positions based on open and advertised positions, then evaluated to the current academic degree programs regarding those required skills. The present study reviewed multiple job advertisements on Yahoo, Google, Monster, Indeed and other HR-advertised locations to determine specific skills organizations expect of potential future employees. A skills list was developed and then presented to both academic and industry participants to establish a set of data for phase I and to obtain feedback from both participant perspectives.

Research Question

R1: Do workforce competencies for employment in a C-Suite level position vary between industry and academicians?

II. Literature Review

CIO, to CSO, to CRO: Employment within the Information Technology (IT) security field

There are many popular and desired upper management and security positions in the areas of Information Technology (IT) Security and Information Systems (IS). Generally, these positions are referred to as the C-Suite field and the more powerful positions are viewed as (*=Security):

- Chief Executive Officer (CEO)
- Chief Financial Officer (CFO)
- Chief Information Officer (CIO) *
- Chief Operating Officer (COO)
- Chief Risk Officer (CRO) *
- Chief Security Officer (CSO) *

The CEO typically has the highest power of the organization and is the leader of the executive team. The CEO's role is to keep the business going. He or she must continually watch for business opportunities, improve efficiency, reduce costs, increase revenue or market share and inspire a vision for the organization [4][5]. The CEO is concerned about organizational success, financial issues, operational processes, and business risk. The CEO position must view the

organization from a bird's eye view to determine why the organization exists and what the ultimate goals are. When it comes to information security, however, the CEO is typically only a part of a team that makes final business and information security decisions and asks questions such as, "Should the information security project be funded? Is this information security strategy a good fit for this organization? Are the costs (i.e. time, money, resources) for the information security project justified? Because of this power, it is imperative that the CEO position has a solid understanding of information security concepts and how they can impact an organization's policies, procedures and goals. The CEO is in need of a tool or method to help him or her make these very critical decisions, and this is where the CIO, CRO, and CSO roles come into play and help to support the executive team.

The CIO is typically the head of the IT Department. The CIO understands how technology can support the business in its quest to reach a specific goal and carry out an identified mission. The CIO must provide IT solutions that help the organization succeed [4][5]. This means that proposed IT projects must be completed on time and within budget. A late IT project or one that goes above the projected budgeted amount can be very detrimental to the organization's success. Whereas, the duties of the CRO differ slightly as they are typically responsible for many of the same duties as the CIO in terms of understanding the corporate landscape and ongoing security projects. However, their field of expertise is more of governance. As data and devices converge, the role of the CRO and their management responsibilities seem to vary across the landscape within the given literature. Nevertheless, the CRO has become a mainstay within the executive leadership team, and according to Karanja and Rosso [6], the CRO provides a voice within three managerial roles: (a) interpersonal, (b) informational, and (c) decisional within the areas of risk control, management, and mitigation.

So, where does the CSO role factor in, one might ask? White papers and research articles focus primarily on the task of the information provider and consultant to the executive team. Papers often include perspective driven solutions, such as (a) present the security solution as a benefit and not a cost, (b) provide statistics that prove the risk is real, and (c) provide examples of real-world incidents [7]. While these are all great communication skills to acquire or have, the business executive finding themselves within the role of CSO should also have some knowledge about conducting risk assessment which aids in the decision-making process. Thus, many that find themselves in high-level business leadership roles are aware of information security risks but they may or may not have full insight into the level of risk they face in order to make informed decisions. Thus, research suggests the need for yet another executive management level simply known as the CISO.

The rise of the Chief Information Security Officer (CISO)

As the use of technology became more of a necessity than a luxury in business, the need for a responsible individual to address the complexities surrounding it increased. The establishment of the Chief Information Officer (CIO) began in the early 1980s [8], but the need for their skills increased over the decades and technology became both proliferous and ubiquitous. The CIO became integral to organizations and soon the CIO was a key player in the day to day workings of almost every organization on the planet. However, this ever-increasing use of technology

brought with it a long list of security risks and challenges. The security risks continued to grow at an alarming pace and the proof became evident as more and more organizations found themselves in the news for yet another security breach. Security breaches not only impact the reputation of an organization but face financial and even legal issues, such as lawsuits. Researchers began to study issues related to information security issues. Standards and frameworks, such as the International Organization of Standardization (ISO), were developed to assist organizations in their struggle to securely manage their information assets. Soon the need for a person in charge of the security of the organization's information system was apparent. However, there was not a clear understanding as to the exact role and responsibilities of the officer in charge [9].

Typically, an organization is led by the Chief Executive Officer (CEO), who is in charge of corporate governance, as well as the major decision making processes, structures and systems [9]. The CEO's main goal is to ensure the success of the organization for the investors and sponsors. CIOs, on the other hand, are concerned with Information Technology (IT) governance, which means they make decisions that ensure the technology of an organization is aligned with the goals and objectives of that organization. Yet, something was still missing and the executive team welcomed the Chief Information Security Officer (CISO) to the table.

In comparison, the CISO is concerned with the governance of information security. He/She is concerned with the security of all IS and IT resources. This can include leadership, communication, processes and any other activities related to security information assets. The CISO is in charge of the security strategy and the security programs while working with all of the business units to ensure alignment. Karanja [9] reported that there is a lack of consensus on the security reporting structure. The most common person that the CISO reported to was the CRO or Legal Officer, followed by the Chief Operating Officer (COO). Each of which, Karanja indicated, was a possible issue with the development of information security best practices. If the COO fails to understand or is not aware of security issues, the proper resources may not be allocated to the security of the information assets. CIO reporting is also a concern. By ensuring the CIO reports to the CEO, the CEO is more likely to be provided a clear picture of the alignment of the technical and business aspects of the organization but miss security concerns.

As mentioned, CEOs are concerned with the overall success of the organization and must rely on the other C-Suite staff for input to assist with organization decisions. Conflict, then,can occur when security governance and corporate governance do not align. As continued adoption of new technology beomes commonplace and the data and device convergence continues to occur, such as cloud services (Software as a Service, Platform as a Service, etc.) the Internet of Things (IoT), a conflict between IT services and IT technology needs complicatesjob roles. To ignore or miss-manage any aspect of these relationships can result in a failed business, the loss of a job, or both.

Fruhlinger [10] reported on eight examples where theCEO, CIOor CSO was fired due to a security breach. He discussed a series of 2016 hacks that occurred at Yahoo. In this example, Yahoo's top lawyer was released from his position, and there were discussions from inside the company to release the CEO, as well. Another cited incident included the Austrian aerospace company FACC. This is a case in which a phishing email was sent including a falsified request

that appeared to come from a very high-level company official to a person with the authority to wire large sums of money. The money was sent and when the dust settled, both the CEO and the CFO were fired.

To further complicate the landscape, another example in which the CSO of the San Francisco State University, who, having a full understanding of the security situation by reporting a vulnerability within their Oracle database structure in comparison to other high-level C-Suite Executives, attempted to provide the best solution for the condition unfolding. However, the executive team overruled and even ignored the request [4]. The security officer presented a solution to the executives to fix the vulnerability but was told it was too expensive. Not long after, a security incident occurred. The executive leaders of the university needed to understand the risk. They needed tools or methods to assess the situation and to determine if the security officer's solutions were the best choice for the situation and the organization.

The information security threat is real and the need for understanding is great in this technological age. Hence, these skills appear to fall outside of the limits or bounds of the CEO, CFO, CRO, and even the CSO, thus, reporting lines have become blurred. Welcome to the rise of the Chief Information Security Officer (CISO).

Work experience and requirements

These incidents are just a small example of the risks that the executive leaders face. Yet, it appears that our academic systems may be failing our future executive leadership team members by not providing proper leadership security training within the curriculum, and as the curriculum is developed, it may be being developed in a vacuum without proper input from industry.

Karanja [9] explains that the reporting structures need to have clear roles and responsibilities. Additionally, each member of the C-Suite must respect and understand these roles and responsibilities. The CISO should focus on the governance of the information security and all aspects that affect the success of the information security program, while the remaining C-Suite members work to ensure the CISO is a respected member of the team. To ensure the CISO can meet the demand of the position, the skills required of the CISO must be clearly understood and academics should work to ensure graduates are fully prepared to fill this critical role.

With this concern in mind, the role of the CISO is greatly needed based upon the many employment ads requesting an executive team member with high-level hands-on skills. The following is a general idea of what an applicant for the role of CISO must possess and are seen as required by most organizations (compiled using Yahoo, Google, Monster, Indeed):

- Work Experience: An applicant to such a position should possess an average of 10 years of experience in the IT security area, with approximately five years of security management and team administration.
- Education: Master's degree, or greater, in IT Security in addition to multiple certificates in the same field.
- Other identified CISO **skills** and **certifications** requirements per employment position listings included:

- C, C++, C#, Java and/or PHP programming languages
- Enterprise architecture
- Firewall and intrusion detection/prevention protocols
- Knowledge of third-party auditing and cloud risk assessment methodologies
- ISO 27002, ITIL and COBIT frameworks
- Network security architecture development and definition
- PCI, HIPAA, NIST, GLBA and SOX compliance assessments
- Practices and methods of IT strategy
- Secure coding practices, ethical hacking and threat modeling
- Security architecture
- Security concepts related to DNS, routing, authentication, VPN, proxy services and DDOS mitigation technologies
- TCP/IP, computer networking, routing and switching
- Windows, UNIX and Linux operating systems

While the previously listed set of skills are key to organizations looking to fill the CISO position, many organizations included certain certifications they deemed crucial for the CISO position. The next section examines the certifications most organizations indicated as important for the CISO position.

Value of IT certifications to the IT security industry to obtain gainful employment

There are three specific employment paths that highlight the navigation through the IS Security path due to convergence. They are (a) CEO, (b) CRO, and (c) CSO as mentioned earlier. As the digital divide has narrowed, so has the C-Suite assignments in terms of security focus and job skill tasks. The CEO was the executive overseeing all levels of information management, but this position has evolved into risk management and governance keeper within the corporation. While this position experienced growth in terms of duties performed such as risk assessment, one position was not enough as the boundaries and infrastructures were penetrated, and the “rise”of hackers began and hence the need for the CISO. Ultimately, these transitions equated to the need for a more security-minded executive to protect assets at all levels, which included data, and personal data at that. Therefore, when viewing employment in this arena, corporations turned their focus to certificate attainment in addition to the educational requirements to ensure those who applied had specific hands-on knowledge of the field.

While hands-on knowledge in relation to certificate attainment still remains under question by some, the testing industry has made great strides in the last decade by including virtualized simulations within the testing environment to showcase hands-on skills. Additionally, certification still remains a necessary artifact to prove skill attainment in addition to degree attainment for current job employment ads. If focusing solely upon the CISO role and based upon current employment job ads, alongside interpersonal communication and organizational skills, both of which appear to be the most frequently requested skills, a CISO should carry some, if not most, of the following certificates:

- CCISO: Certified Chief Information Security Officer
- CGEIT: Certified in the Governance of Enterprise IT

- CISA: Certified Information Systems Auditor
- CISM: Certified Information Security Manager
- CISSP: Certified Information Systems Security Professional
- CISSP-ISSMP: Information Systems Security Management Professional

To achieve certification, much study preparation and time on task with regard to professional experience is very much in demand. Depending upon the certification exam and application process, applicants are required to not only pay to sit the required exam but must provide proof of professional work experience in the specific field or domain prior to exam application. The following provides an overview of the two most predominant certifications related to those employed or seeking employment as a CISO. These certificates include: (a) CISSP and (b) CISM [11].

Per $(ISC)^2$ online guidance [12], "Candidates must have a minimum of five years cumulative, paid, full-time work experience in two or more of the eight domains of the CISP Common Body of Knowledge (CBK)"(p. 3), with a one-year exemption for education. Per the 13-page "Ultimate Guide," the history of the CISSP began in 1994, is accepted by the Department of Defense (DOD), meets the ISO/ICE Standard 17024, and became adaptive via computerization only in 2017. While the exam is expected to take a maximum of three hours due to the almost 150 questions asked, the topics range from Security and Risk Management to Software Development, and include identity management and architecture elements.

In contrast, the CISM is managed by ISACA (now goes by the acronym only). This exam is a 200-question exam that explores the "testers" knowledge of security, risk management, compliance, security program development, and management and incident handling. Again, this certification requires five years of field experience and indicates that this experience must be gained via the last 10 years prior to the examination. However, and more importantly, three of the five years of experience must be in management. The value appears to remain on the ability to prove hands-on experience, and thus, does not rely on theory nor book smarts alone, yet, pure workforce abilities for said topic.

Due to specific skill set requirements for those filling any position within the C-Suite role, certification is not enough. Academic programs must alignment to support this need. With this knowledge, academics who construct courses and programs within the field must take notice of the overwhelming need for hands-on skills. This condition equates then to the need for the curriculum to also present said challenges for learning and provide for conditions in which to master workforce skills and pass the needed certification exams while earning a college degree. This then turns the focus upon the academic programs that are created to support this pathway. Thus, a framework in which to examine this alignment is needed. The focus of this current research study is to present a framework in which to support this academic to industry training alignment and investigation.

III. Methods Section

Theoretical framework

Based on Developing A CUrriculuM (DACUM) theoretical framework [13], one that compares academics to workforce preparatory needs, a newly constructed framework was formulated for this current study. The DACUM method utilizes a step-by-step process that includes expert workers who explain their job tasks, roles, and skill set requirements, which is a direct implication of knowledge and skills the workers must-have. Using the DACUM approach and guidance, researchers posit the following framework "From Degree to CISO Employment" which is displayed in *Figure 1*: Degree to CISO Employment Framework. This framework examines the perspectives of the current workforce and identifies requirements that academicians can address to ensure a well-rounded academic program is constructed to meet the needs of the identified workforce positions.

Also entwined within this framework's construction is the seminal, socio-technical Leavitt Diamond theoretical framework [14], which addresses the workforce relationships between (a) **People**, (b) **Process**, (c) **Technology**, and (d) **Structure** and how each construct impacts the other [15]. For this study, the structure portion of the model includes the C-Suite personnel who work within one of the following four structural business models, or a combination thereof: (a) **Financial**, (b) **Service-oriented**, (c) **Strategy-based**, and (d) **Technological**. The posited framework suggests that within the curriculum development process, both Academicians and Industry members, particularly those employed at the C-Suite level, be surveyed at an established interval to ascertain and collect the most current skills or certifications needs that are either being taught or required to secure gainful employment within the C-Suite field. It is further suggested within this framework that the development process includes qualitative discussions or focus groups on a continual rotation with upper-level C-Suite Executives to explore and disseminate these findings as displayed in *Figure 1*: Degree to CISO Employment Framework.

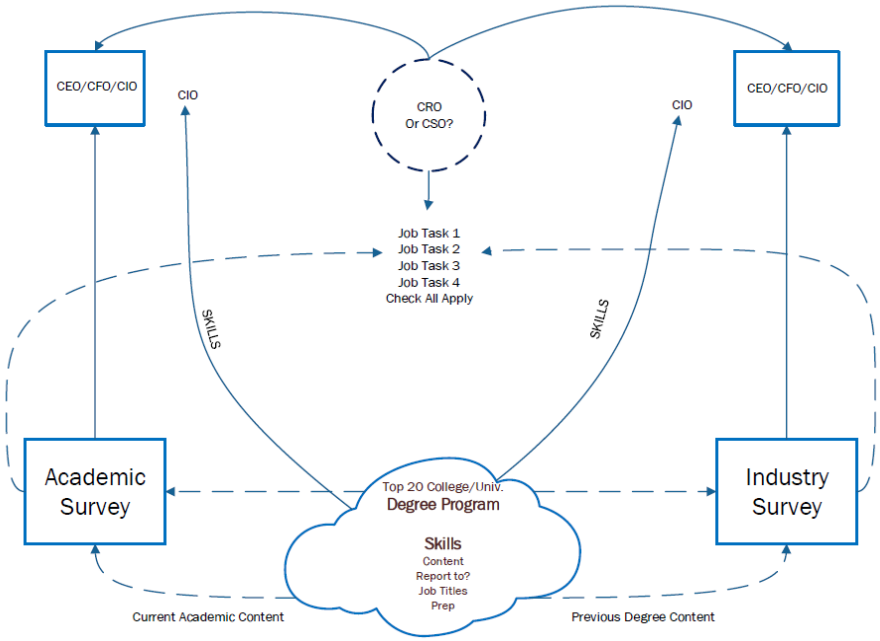

Figure 1: Degree to CISO Employment Framework

Figure 1: Degree to CISO Employment Framework displays the flow of the overall process that begins by examining the academic program (Academicians) under investigation to that of C-

Suite (Industry) members and their previous academic training. Each participant is provided a separate survey that addresses either a current academic perspective or a current workforce perspective on the required skills of the position. The C-Suite participants indicate if their required job competencies were previously learned or if they were obtained after graduation. Each survey includes a skill listing for each C-Suite position with the participant ranking the skills for each. The corporate reporting structure of the C-Suite positions is also collected within the Industry portion of this framework and survey collection process. It is expected that the Academicians will report their current employment rank, the degree programs offered at their institution, and whether the offered degrees and degree structure addresses skills needed to obtain industry certification, if any, that may be embedded within their curriculum. This process allows the researchers to conduct an analysis of the gaps between priorities of current academic programs, the skills taught, and applicability to the workforce.

Method

A modified Delphi approach was selected as the method to ascertain and examine the skills gap, if any, between academic training to that of employment requirements. Normally within a Delphi study, elements of comparison are created via opinions gathered from a diverse, yet expert-level panel, and then ranked over a series of ranking events. The group facilitator would normally select a group of experts based on the topic being examined. After membership in the Delphi study has been confirmed, each participant would normally receive a questionnaire and provide qualitative data regarding the subject matter or materials under examination, or comment about research in the field in which to create a skills listing survey to rank. This phase is typically used to gather data from the experts, and then summarize their points of interest in which to allow for voting or ranking, but begins with the facilitator organizing collected data to create a listing output to conduct a series of ranking events until a consensus is reached.
However, within this modified approach, and due to this being Phase I of a multi-phased research examination, the initial element listing was constructed using common employment outlets, such as Yahoo, Google, Monster, Indeed, and those employment skill requirements as found within the current literature. Additionally, the listing was further delineated by common functionality dimensions discussed within the above *Theoretical Framework* section as to how IT-related employment positions can transverse the various four-dimension model including (a) People, (b) Process, (c) Technology, and (d) Structure. Thus, two versions of a Delphi-based ranked survey were available. One for Industry members, and the other for Academicians.

Surveys were intended to compare and rank required competencies of C-Suite employment positions between members of the workforce, referred to as Industry, and those who are preparing students to enter the said workforce referred to Academicians. Surveys contained correlation elements between employment titles, academic ranking, degrees obtained, and corporate reporting structures with open-ended elements where needed for the expansion of discussion. It should be noted that the ranked components found within each survey are the same with only demographic questioning avenues and other feedback requests differing between the two surveys. Questionnaire ranking segments can be found in *Appendix A* for further review.

Whereas, *Appendix B* and *C* provide a copy of each survey, Industry and Academicians, for detailed review.

Within the current examination, the primary research concerns, other than to answer the intended research question, were that of the survey construction based upon employment ad generated data, and participant feedback regarding the climate of the C-Suite field or other areas in which future examinations should focus. Thus, a limited sample was used from one academic program, that gathered data to support the investigation the applicability of the skill employment listings that were created prior to the study rather than using experts in which to construct each survey. Thus, interviews have yet to be scheduled in which to reach a consensus regarding the ranked materials. However, qualitative data was reviewed in which to create a foundation or note additional concerns in which to investigate. These data and findings will be briefly sharing under the *Data Collection and Analysis* section of this paper.

Lastly, it should be noted that according to Twin [16], due to this being a Delphi study, response times tend to differ and the value of information can be limited. Thus, researchers approached the analysis with no expectations other than the desire to gather data to support the foundational phase of the project in terms of sample, instrumentation validity and reliability, and to identify educational skill alignment and competencies of those employed within the C-Suite arena in comparison to Academicians.

Sample and context

Respondents were selected based upon their teaching assignment at a small, private institution in the southeast United States. A total of 21 faculty members, both Adjunct and Full-time, from the Management of Information Security and Assurance (MISA) program were invited via email to take part in this initial two-survey validation effort. This was a volunteer recruitment effort in which Faculty self-selected which survey to complete based upon their affinity to either academics or industry within the IS and the security fields. Of those invited, five members (n=5) members in total responded to the surveys and provided qualitative feedback in which to review. The sample yielded an overall 24% response rate with 10% (n=2) and 14% (n=3) between Academicians and Industry respectively. Due to the anonymous nature of the survey process to support validation needs, it is possible that members may have sat both versions of the survey as it was an open selection based upon the respondent's choice.

IV. Data Collection, Analysis, and Discussion

The following section intends to not only display and present findings based upon collected survey data but will discuss findings in support of answering *Research Question 1 - Do workforce competencies for employment in a C-Suite level position vary between industry and academicians?* While qualitative feedback was collected, it was done so to collect statements that demonstrate the current climate as viewed by each respondent. Thus, a thematic analysis was not conducted.

Demographics

The survey group consisted of Adjuncts and Full-time Faculty members across one security program (n=5), who indicated having PhDs (n=2, disciplines not provided) and the degrees of DM/IST (n=2) and DBA (n=1). Of those sitting the Industry version of the Delphi-ranked survey, they indicated that they hold the titles of (a) CISO (n=1), (b) CRO (n=1), and (c) Other – Lead Cyber Security Engineer (n=1). Lastly, reporting structures of the industry respondents (n=3), who indicating as working for corporations hosting Service-oriented or combination operating models, appeared to support a one-dimensional reporting structure reporting to the CEO of their respective employers. Whereas, only one respondent indicated that they reported to "Other" due to being employed by an organization that operated within a matrix system that includes multi-reporting lines. Thus, findings somewhat negate the literature in terms of varying or lack consistency in reporting structures [1][6] and remains a viable venue and topic for future research efforts.

Certifications

As reported by the respondents, academic institutions do attempt to correlate degree offering content to that of certification requirements as seen in *Figure 2*: Importance of Certifications to Degree Programs. Degrees support certificates of CCISO, CISO, and CISSP according to the Academicians surveyed. However, it is important to note, the more popular industry-accepted certification, CISM, was not a focus within the current curriculum landscape as reported by the respondents. Thus, a contradictory finding negating the literature [11].

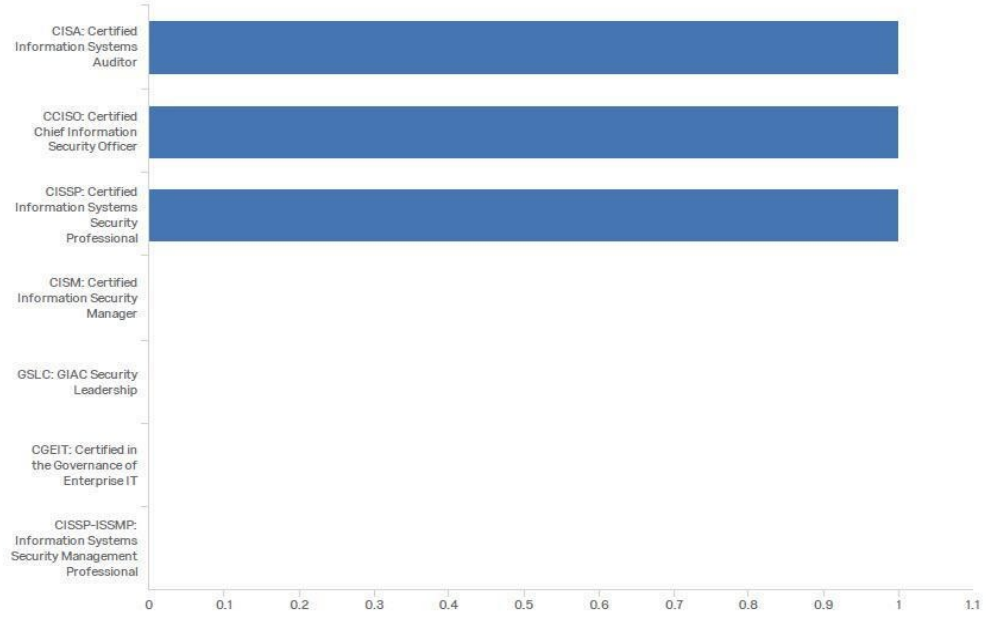

Figure 2: Importance of Certifications to Degree Programs

As seen in *Figure 3*: Certification to C-Suite Employment by Requirement, when asked to rank by certification importance for employment, a true consensus could not be derived. However, the Certified Chief Information Security Officer (CCISO), Certified Informaiton Systems Audtidor (CISA), Certified Information Systems Security Professional (CISSP), and the GIAC Security Leadership Certification (GSLC) [17], were the certifications to be ranked as number one in

importance to obtain, whether as “Required” or “Preferred.” However, there was no agreement between the top three ranked categories in order of importance for any such certificate, but the CISSP ranked both first and third in the area of ranking order of importance (n=1, n=1 respectively).

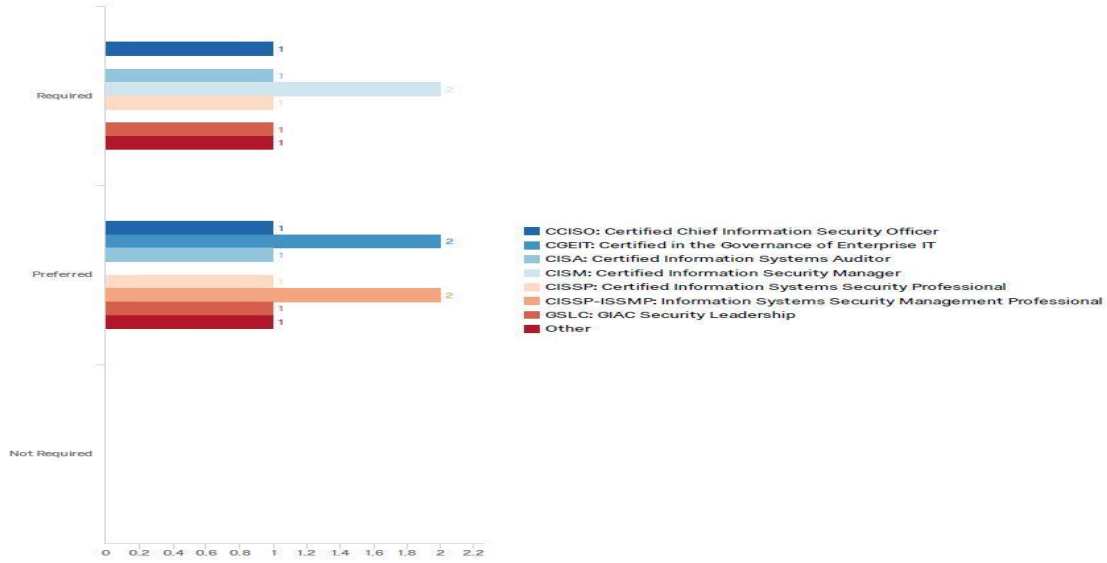

Figure 3: Certification to C-Suite Employment by Requirement

Helpful for workforce preparation –Industry survey response

When examining the tri-focus business framework in support of identifying helpful skills for preparing and securing employment within the C-Suite arena, there were only six employment skills found to be *Helpful* to *Somewhat Helpful*, as seen with *Figures 4-6* pertaining to (a) People (*Figure 4*), (b) Process (*Figure 5*), and (c) Technology (*Figure 6*). They are:

- Act as a liaison to the information systems and compliance departments
- Ability to oversee developing and delivery of initial and ongoing security training to the workforce
- Ability to assess third party security requirements (* one respondent identified as Very Helpful)
- Manage the development and implementation of the global security policy, standards, guidelines and procedures
- Ensure organizational audit controls monitor activity on electronic systems that contain or use protected personal information
- Safeguard physical security of the organization, to include asset protection, workplace violence prevention, access control systems, video surveillance, and alike systems

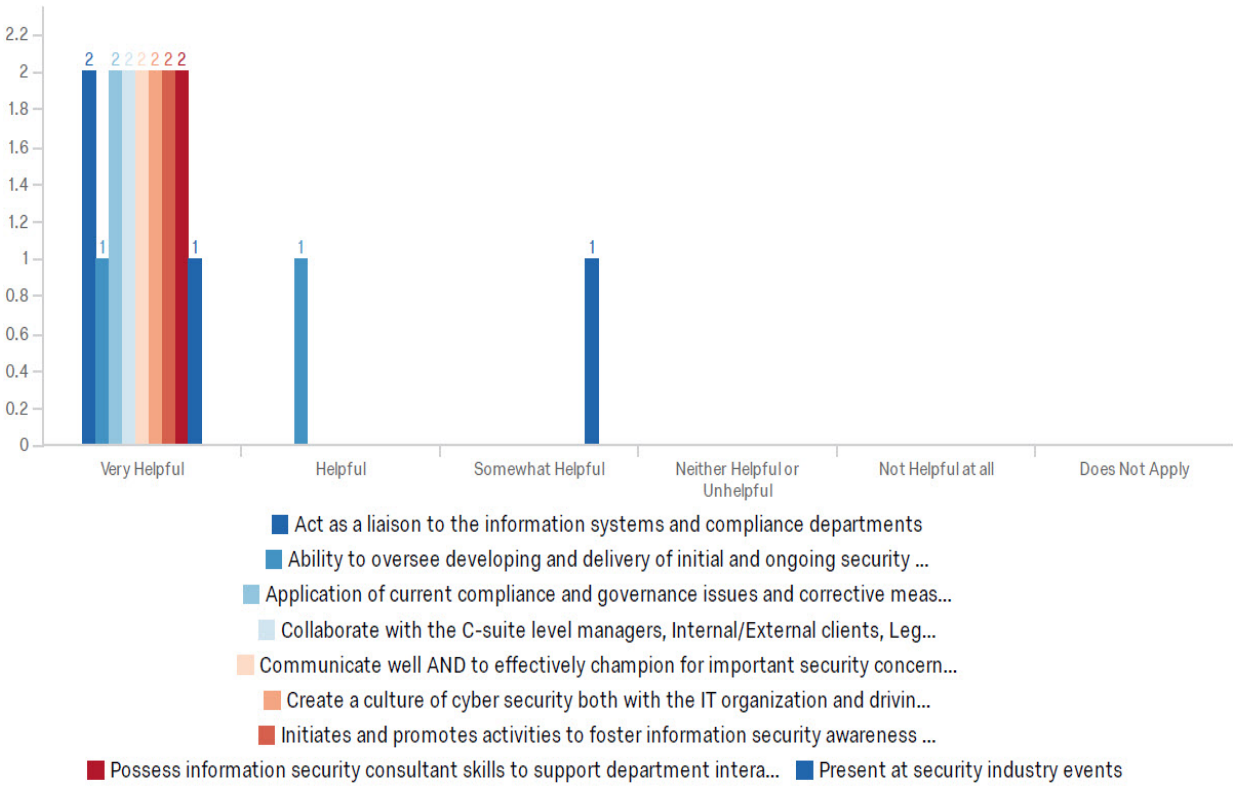

Figure 4: Helpful Skills by People Dimension

Figure 5: Helpful Skills by Process Dimension

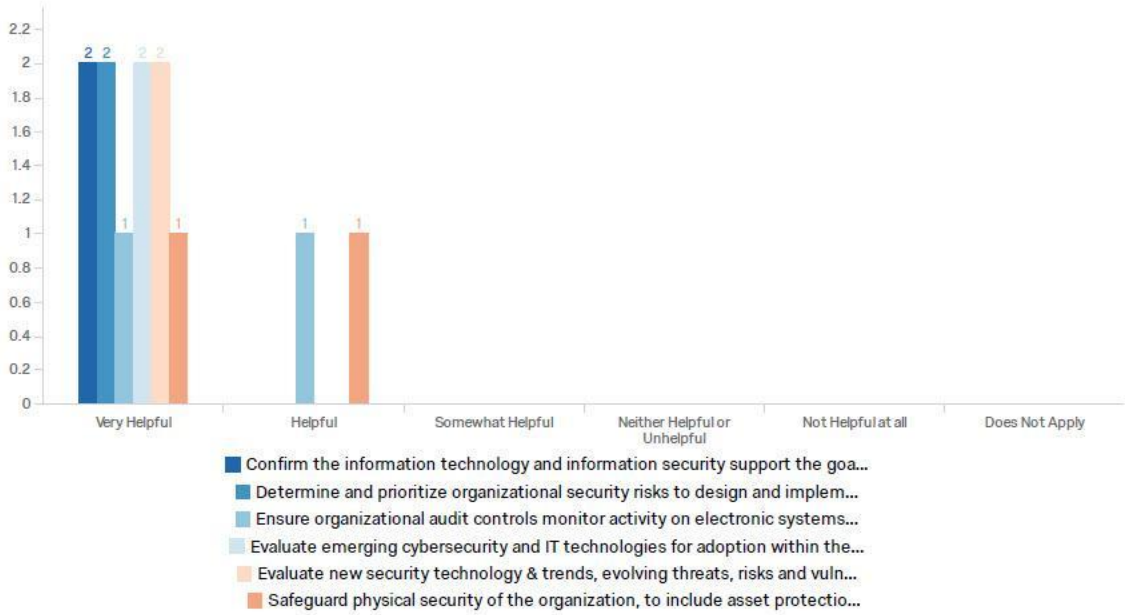

Figure 6: Helpful Skills by Technology Dimension

Order of importance in current role

When ranked by order of importance under the dimenson of *People*, some conflicts were witnessed, which was expected. However, no skill was considered unimportant. There was only one ranking, Rank 6, in which both respondents agreed that "Application of current compliance and governance issues and corrective measures (regulatory mandates, including PCI DSS, SOC 2 Type II, GDPR, HITRUST, and more" should rank as sixth in importance. The top three ranks for *People* can be seen in Table 1.

Table 1

C-Suite Skill Ranked Differences by Dimension: People

Ranking	By Skill
1	Collaborate with the C-Suite level managers, Internal/External clients, Legal Department, organizational senior management, and Subject Matter Experts (SMEs) Create a culture of cyber security both with the IT organization and driving behavioral changes for the business
2	Communicate well AND to effectively champion for important security concern protections Create a culture of cyber security both with the IT organization and driving behavioral changes for the business

3	Initiates and promotes activities to foster information security awareness within the organization and related entities
	Possess information security consultant skills to support department interaction to properly identify all data security related issues and needs

Whereas, if viewing results for the dimension of *Process*, respondents agreed with the ranking order of Rank 1, 3, 5, and 6. The top three ranks for *Process* can be seen in Table 2. However, three skills were seen as not being applicable: (a) Manage breach determination and notification processes under privacy laws and applicable State breach rules and requirements, (b) Establishing and administer processes for security breaches, and (c) Monitor compliance of all vendor agreements to ensure security concerns, requirements, and responsibilities are addressed.

Table 2

C-Suite Skill Ranked Differences by Dimension: Process

Ranking	By Skill
1	Ability to assess third party security requirements
	Develop and implement a security risk management plan
2	Develop and managing organizational budgets
	Manage the development and implementation of the global security policy, standards, guidelines and procedures
3	Maintain information security policies, standards, and procedures

Lastly, if speaking of the ranked order for *Technology*, no ranks were in agreement and the top three ranks for *Technology* are seen in Table 3. It should be noted that "Safeguard physical security of the organization, to include asset protection, workplace violence prevention, access control systems, video surveillance, and alike systems" was identified as a skill that no longer applies (n=1). This suggests a view in which physical security no longer plays a vital role in the infrastructure as it once did, possibly in lieu of cloud-computer security needs.

Table 3

C-Suite Skill Ranked Differences by Dimension: Technology

Ranking	By Skill
1	Evaluate new security technology & trends, evolving threats, risks and vulnerabilities and provides recommendations to strengthen internal and external information security environment
	Safeguard physical security of the organization, to include asset protection, workplace violence prevention, access control systems, video surveillance, and alike systems
2	Determine and prioritize organizational security risks to design and implement information security controls
	Ensure organizational audit controls monitor activity on electronic systems that contain or use protected personal information
3	Confirm the information technology and information security support the goals and objectives of the organization.
	Ensure organizational audit controls monitor activity on electronic systems that contain or use protected personal information

Academic views of prioritization of C-Suite skills

In comparison to the Industry ranking efforts, Academicians were also asked to rank skill set requirements in comparison to specific C-Suite Executive positions. Based on the literature examined, only the following top-tier C-Suite Executive positions results will be displayed: CEO, CSO, and CIO. Those skills that tied in rank are indicated with a (*).

The top rankings for the CEO position were:

- People: (a) Create a culture of cyber security both with the IT organization and driving behavioral changes for the business, (b) Communicate well AND to effectively champion for important security concern protections, and (c) Collaborate with the C-Suite level managers, Internal/External clients, Legal Department, organizational senior management, and Subject Matter Experts (SMEs)
- Process: (a) Develop and manage organizational budgets, (b) *Maintain information security policies, standards, and procedures, * Manage the development and implementation of the global security policy, standards, guidelines and procedures, and (c) Develop and implement a security risk management plan
- Technology: (a) * Develop and implement a security risk management plan, *Develop and managing organizational budgets, (b) *Ability to assess third party security

requirements, *Develop and implement a security risk management plan, and (c) *Address disaster recovery, business continuity, risk management and access control needs of the company, *Manage the development and implementation of the global security policy, standards, guidelines and procedures

The top rankings for the CSO position were:

- People: (a) *Collaborate with the C-suite level managers, Internal/External clients, Legal Department, organizational senior management, and Subject Matter Experts (SMEs), *Create a culture of cyber security both with the IT organization and driving behavioral changes for the business, (b) *Act as a liaison to the information systems and compliance departments, *Initiates and promotes activities to foster information security awareness within the organization and related entities, (c) *Communicate well AND to effectively champion for important security concern protections, *Possess information security consultant skills to support department interaction to properly identify all data security related issues and needs
- Process:(a) *Develop and implement a security risk management plan, *Manage the development and implementation of global security policy, standards, guidelines and procedures, (b) *Establishing and administer processes for security breaches, *Develop and implement a security risk management plan, (c) *Address disaster recovery, business continuity, risk management and access controls needs of the company, *Maintain information security policies, standards, and procedures
- Technology:· (a) *Develop and implement a security risk management plan, *Manage the development and implementation of global security policy, standards, guidelines and procedures, (b) *Develop and implement a security risk management plan, *Develop and managing organizational budgets, (c) *Address disaster recovery, *Business continuity, risk management and access controls needs of the company

The top rankings for the CIO position were:

- People: (a) * Collaborate with C-Suite level managers, internal/external clients, legal department, organizational senior management, and subject matter experts (SMEs), *Application of current compliance and governance issues and corrective measures (regulatory mandates, including PCI DSS, SOC 2 Type II, GDPR, HITRUST, and more), (b) * Act as a liaison to the information systems and compliance departments, * Ability to oversee developing and delivery of initial and ongoing security training to the workforce, and (c) *Act as a liaison to the information systems and compliance departments, *Ability to oversee developing and delivery of initial and ongoing security training to the workforce
- Process: (a) * Manage breach determination and notification processes under privacy laws and applicable State breach rules and requirements, * Maintain information security policies, standards, and procedures, (b) * Develop and implement a security risk management plan, *Ability to assess third party security requirements, and (c) *Manage breach determination and notification processes under privacy laws and applicable State

breach rules and requirements, *Manage the development and implementation of the global security policy, standards, guidelines and procedures

- Technology: (a) *Develop and implement a security risk management plan, *Ability to assess third party security requirements, (b) *Address disaster recovery, business continuity, risk management and access control needs of the company, *Manage breach determination and notification processes under privacy laws and applicable State breach rules and requirements, and (c) *Address disaster recovery, business continuity, risk management and access control needs of the company, *Develop and Manage organizational budgets

All-in-all, it appears the two groups were largely in agreement when identifying needed skills across the *People* and *Process* dimensions. However, only the role of CIO stood out as needing other, more specific workforce skills as perceived by the Academicians as they placed higher importance on governance and compliance, and risk planning and reporting. Whereas, the largest discrepancy by dimension can be found within the *Technology* dimension across all C-Suite positions and identified skills. The variance showcased the need for development efforts on the part of the CIO while addressing business continuity, risk management overall, and budgetary concerns.

Employment skills not needed by graduates

In comparison to industry perspectives and responses, Academicians perceived the skills needed for the C-Suite Executives to be viewed only in a different format with ranks varying. Thus, this may shed light on perceived curriculum differences, if any, when examining student preparatory needs. Whereas, the hosting of iterative discussions or focus groups would be supportive in helping to create a consensus between views. While it is important to note that all skills were examined by both Industry and Academicians as they apply to employment needs, it is equally important to identify skills that are considered to be no longer needed by graduates. This would suggest that these skills should no longer be embedded in the current curriculum or curriculum development process moving forward. Those skills included: (a) PCI, HIPAA, NIST, GLBA and SOX compliance assessments, (b) Practices and methods of IT strategy, (c) Security concepts related to DNS, routing, authentication, VPN, proxy services and DDOS mitigation technologies, and (d) Windows, UNIX and Linux operating systems. Of particular notice, the skills statement of "C, C++, C#, Java and/or PHP programming languages" appeared to have no bearing within the ranking event as it was not selected by any of the respondents. Oddly, these skills relate to government compliance, coding, and hands-on networking elements all of which are required skills needed to manage server access and skills needed to uphold the CIA security computing triad in support of Confidentiality (C), Integrity (I), and Availability (A).

Lastly, the following skills under the various dimension areas were either identified as least important or having no bearing upon the ranked event. Those skills included: (a) Initiates and promotes activities to foster information security awareness within the organization and related entities (People), (b) Present at security industry events (People; Not Ranked), (c) Address disaster recovery, business continuity, risk management, and access controls needs of the company (Process), (d) Develop and implement a security risk management plan (Process), (e)

Monitor compliance of all vendor agreements to ensure security concerns, requirements, and responsibilities are addressed (Process), and (f) Safeguard physical security of the organization, to include asset protection, workplace violence prevention, access control systems, video surveillance, and alike systems (Technology). Another oddity with regard to these findings as the data suggests that end-user training, making the end-user aware of the many types and tactics surrounding security breaches, and the sharing of information breaches through publication and presentation across disciplines, all appear to negate options to support awareness and the investigation of security behaviors which may be seen as the best line of defense in preventing future breaches.

Additional qualitative feedback shared

- "Fully understand the business mission, vision, values, and strategic plan. Be able to design and optimize an Enterprise Risk Management Plan which helps the business fulfill its mission, is in line with its vision and values, and assists it meet its strategic goals."
- "For government related contracts, one of the skills needed to some knowledge of the organization or related work. Additionally, knowledge or qualification to serve in many areas requires a security clearance or background check. Although the clearance is not a skill, it limits the workforce and may be worth exploring from intern program opportunities."
- "CISO's need to be well rounded, in both Business Administration and Security (Risk, Controls, Regulations, etc.). Best bet, develop a DBA concentration (i.e., DBA/Risk Management) to foster this symbiotic relationship. The Business takes precedent - the business can exist without security (and, sadly does at times), but security cannot exist without the business."
- "I have not found that many organizations are maximizing the CISO position. It would be interesting to understand the roles of the CTO, CIO, and CISO and how the C-Suite prefers or rank orders these positions."

V. Conclusion and future work

Overall, while there are slight differences seen between Industry and Academicians in their various views while ranking order of importance, and certification attainment based upon curriculum construction in support of required needed skills found within the workforce, there are many avenues in which the two respondent categories did agree. The researchers suggest that Industry and Academicians need to collaborate more to compare the ever-changing skills of the field as they relate or need updating based upon changes to technology, the landscape, computing power, and to identify those skills that have become outdated due to these changes.

However, respondents also suggest the need for future investigation in the area of the importance of each role expanding to include the role of the Chief Technology Officer (CTO). While important to include the CTO within these discussions, the authors suggest that future investigations initially focus upon reporting structures and order of importance in rank but begin with the analysis of the new emerging role, the CISO, in hopes to further bridge the gap between the CEO to CSO, to that of the CSO to CIO to create a more supportive environment that

includes role clarification while supporting the views of both the corporate structure as technology continues to converge on all sides and that of degree and certification employment requirements.

References

[1] R. D. Banker, N. Hu, P. A. Pavlou, and J. Luftman, "CIO reporting structure, strategic positioning, and firm performance," *MIS Quarterly*, 35(2), pp. 487-504, 2011.

[2] I. Halasz, "Overview of the DACUM Job Analysis Process," US Department of Justice, National Institute of Corrections, NIC Academy. Report , Report 199-I, September 1-3, 1994.

[3] K. Ki-Yoon and K. Surendran, "Information security management curriculum design: A joint industry and academic effort," Journal of Information Systems Education, 13(3), pp. 227, 2002.

[4] T. Fitzgerald, "Clarifying the roles of information security: 13 questions the CEO, CIO, and CISO must ask each other," Information Systems Security, 16(5), pp. 257-263, 2007. doi: 10.1080/10658980701746577.

[5] T. Fitzgerald, CISO compass navigating Cybersecurity leadership challenge with insights from pioneers, 2019. [E-reader Version]. doi: 10.1201/9780429399015

[6] E. Karanja and M. A. Rosso, "The Chief Risk Officer: a study of roles and responsibilities," Risk Management, 19(2), pp. 103-130, 2017.

[7] Barkly Protects, Inc., "Budget and buy-in: Getting executive invested in cybersecurity," *Hubspot*, 2018. [Online]. Available: Hubspot, https://cdn2.hubspot.net/hubfs/468115/eBooks/getting-execs-invested-cybersecurity/barkly-getting-executives-invested-in-cybersecurity.pdf?t=1532924238737 [Access Jan. 6, 2020].

[8] T. May, "Evolution of the CIO: The real story," Computer World, Jan. 6, 2016. [Online]. Available: Computer World, https://www.computerworld.com/article/3019768/evolution-of-the-cio-the-real-story.html [Access Jan. 6, 2020].

[9] E. Karanja, "The role of the chief information security officer in the management of IT security," Information & Computer Security, 25(3), pp. 300-329, 2016.

[10] J. Fruhlinger, "The buck stops here: eight security breaches that got someone fired," CSOnline, Dec. 6, 2017. [online]. Available: CSOnline, https://www.csoonline.com/article/2859485/data-breach/the-buck-stops-here-8-security-breaches-that-got-someone-fired.html#slide1 [Access Jan. 6, 2020].

[11] J. Petters, "CISM vs. CISSP Certification: Which one is best for you?," [Online] Available: Varonis, https://www.varonis.com/blog/cism-vs-cissp/. [Accessed Jan. 6, 2020].

[12] ISC2, The ultimate guide to the CISSP. How to achieve the world's premier cybersecurity certification. ISC2, 2019. [E-book] Available: ISC2, https://www.isc2.org/-/media/ISC2/Certifications/Ultimate-Guides/UltimateGuideCISSP-Web.ashx?la=en&hash=E98F3E3FFFD76FEE18154D3C2A135D68806AE69B

[13] L. Halawi, W. M. Kappers, and A. Glassman, "From enrollment to employment: A DACUM approach to Information Systems and Information Security and Assurance curriculum design," Issues in Information Systems, 17(3), pp. 218-226, 2016.

[14] H. Leavitt, Applying organizational change in industry: Structural, technical, and humanistic approaches. Handbook of organizations, Chicago, IL: Rand McNally, 1965.

[15] M. Harrell, "Synergistic Security: A work system case study of the Target breach," Journal of Cybersecurity Education, Research & Practice, 2017(2), pp.1-23, 2017.

[16] A. Twin, "Delphi method," Investopedia, June 25, 2019. [Online]. Available: Investopedia, https://www.investopedia.com/terms/d/delphi-method.asp [Accessed Jan. 6, 2020].

[17] GIAC, "Cyber Security Certification: GSLC," (n.d.), [Online] Available: GIAC, https://www.giac.org/certification/security-leadership-gslc [Access Jan. 25, 2020].

Appendix A

Common Ranked Elements between Surveys

1. **Dimension**: PEOPLE
    a. Act as a liaison to the information systems and compliance departments
    b. Ability to oversee developing and delivery of initial and ongoing security training to the workforce
    c. Application of current compliance and governance issues and corrective measures (regulatory mandates, including PCI DSS, SOC 2 Type II, GDPR, HITRUST, and more
    d. Collaborate with the C-Suite level managers, Internal/External clients, Legal Department, organizational senior management, and Subject Matter Experts (SMEs) to:
        i. Create and maintain a strategic and comprehension security program
        ii. Ensure alignment between security and privacy compliance programs including policies, practices and investigations
        iii. Establish governance for the corporate-wide security program, including physical and electronic assets
        iv. Identify business requirements and implement people, process, technology, and/or oversight/governance to achieve desired outcome(s)
    e. Communicate well AND to effectively champion for important security concern protections
    f. Create a culture of cyber security both with the IT organization and driving behavioral changes for the business
    g. Initiates and promotes activities to foster information security awareness within the organization and related entities
    h. Possess information security consultant skills to support department interaction the
    i. Present at security industry events
2. **Dimension**: PROCESS
    a. Ability to assess third party security requirements
    b. Address disaster recovery, business continuity, risk management and access controls needs of the company
    c. Manage breach determination and notification processes under privacy laws and applicable State breach rules and requirements
    d. Establishing and administer processes for security breaches
    e. Develop and implement a security risk management plan
    f. Develop and managing organizational budgets
    g. Maintain information security policies, standards, and procedures
    h. Manage the development and implementation of the global security policy, standards, guidelines and procedures
    i. Monitor compliance of all vendor agreements to ensure security concerns, requirements, and responsibilities are addressed

3. **Dimension**: TECHNOLOGY
    a. Confirm the information technology and information security support the goals and objectives of the organization
    b. Determine and prioritize organizational security risks to design and implement information security controls
    c. Ensure organizational audit controls monitor activity on electronic systems that contain or use protected personal information
    d. Evaluate emerging cybersecurity and IT technologies for adoption within the organization, as well as provide guidance to sales and engineering teams
    e. Evaluate new security technology & trends, evolving threats, risks and vulnerabilities and provides recommendations to strengthen internal and external information security environment
    f. Safeguard physical security of the organization, to include asset protection, workplace violence prevention, access control systems, video surveillance, and alike systems

Appendix B

"C" Suite Survey - Industry

"C" Suite Survey – Industry

I. Please indicate your highest degree level obtained (**checkbox**)
   a. None
   b. Associates
   c. Bachelors
   d. Masters
   e. EdD
   f. PhD
   g. Other_List

II. Indicate Your Title (**checkbox**)
   a. CEO (Chief Executive Officer)
   b. CFO (Chief Financial Officer)
   c. CIO (Chief Information Officer)
   d. CISO (Chief Information Security Officer)
   e. CRO (Chief Risk Officer)
   f. CSO (Chief Security Officer)
   g. Other_List

III. Who Do Your Report To (**checkbox**)
   a. CEO (Chief Executive Officer)
   b. CFO (Chief Financial Officer)
   c. CIO (Chief Information Officer)
   d. CISO (Chief Information Security Officer)
   e. CRO (Chief Risk Officer)
   f. CSO (Chief Security Officer)
   g. Other_List

IV. Typically, corporations operate under one of four structural business models to support their mission and vision of their corporation: (a) **Financial**, (b) **Service-oriented**, (c) **Strategy-based**, and (d) **Technological**. Based upon the operating model selected, reporting and organization structures are created to support this focus. To examine this alignment in relation to "C" Suite positions, based upon your reporting line as indicated in Question II, please indicate your corporation's business model (e.g. I am a CISO and report to the CEO): (**checkbox**)
   a. Financial
   b. Service-oriented
   c. Strategy-based
   d. Technological
   e. Combination __List
   f. Other __ List

V. The following survey areas, Questions V - VIII, identify required "C" Suite employment skills. This listing was derived from common employment job posting boards, such as Salary.com, Monster.com, and Indeed.com (etc.) with the listing being further reduced and compressed by the researchers to remove repetitive and redundant statements. Further each ranked question is divided into three question dimensions: (a) **People**, (b) **Process**, and (c) **Technology**. Each question should be answer based upon indicated question focus found in bold.

On a scale from 1-5, with five being the highest, which skills were **helpful in *PREPARING* you for your current role**? If the skills does not apply, select "Does Not Apply." **(Likert Scale)**

a. ***PEOPLE***
   i. Act as a liaison to the information systems and compliance departments
   ii. Ability to oversee developing and delivery of initial and ongoing security training to the workforce.
   iii. Application of current compliance and governance issues and corrective measures (regulatory mandates, including PCI DSS, SOC 2 Type II, GDPR, HITRUST, and more.
   iv. Collaborate with the C-suite level managers, Internal/External clients, Legal Department, organizational senior management, and Subject Matter Experts (SMEs) to:
      1. Create and maintain a strategic and comprehension security program
      2. Ensure alignment between security and privacy compliance programs including policies, practices and investigations
      3. Establish governance for the corporate-wide security program, including physical and electronic assets
      4. Identify business requirements and implement people, process, technology, and/or oversight/governance to achieve desired outcome(s)
   v. Communicate well AND to effectively champion for important security concern protections
   vi. Create a culture of cyber security both with the IT organization and driving behavioral changes for the business
   vii. Initiates and promotes activities to foster information security awareness within the organization and related entities
   viii. Possess information security consultant skills to support department interaction to properly identify all data security related issues and needs
   ix. Present at security industry events

b. ***PROCESS***
   i. Ability to assess third party security requirements
   ii. Address disaster recovery, business continuity, risk management and access controls needs of the company
   iii. Manage breach determination and notification processes under privacy laws and applicable State breach rules and requirements
   iv. Establishing and administer processes for security breaches
   v. Develop and implement a security risk management plan
   vi. Develop and managing organizational budgets
   vii. Maintain information security policies, standards, and procedures
   viii. Manage the development and implementation of the global security policy, standards, guidelines and procedures
   ix. Monitor compliance of all vendor agreements to ensure security concerns, requirements, and responsibilities are addressed

c. ***TECHNOLOGY***

i. Confirm the information technology and information security support the goals and objectives of the organization.
ii. Determine and prioritize organizational security risks to design and implement information security controls
iii. Ensure organizational audit controls monitor activity on electronic systems that contain or use protected personal information
iv. Evaluate emerging cybersecurity and IT technologies for adoption within the organization, as well as provide guidance to sales and engineering teams
v. Evaluate new security technology & trends, evolving threats, risks and vulnerabilities and provides recommendations to strengthen internal and external information security environment
vi. Safeguard physical security of the organization, to include asset protection, workplace violence prevention, access control systems, video surveillance, and alike systems

VI. Based upon your current job role, please **rank** these skills in **order of** ***IMPORTANCE TO YOUR JOB TITLE.*** If the skill(s) does not apply simply do not select the skill option. (**ranking exercise**)

d. ***PEOPLE***

i. Act as a liaison to the information systems and compliance departments
ii. Ability to oversee developing and delivery of initial and ongoing security training to the workforce.
iii. Application of current compliance and governance issues and corrective measures (regulatory mandates, including PCI DSS, SOC 2 Type II, GDPR, HITRUST, and more.
iv. Collaborate with the C-suite level managers, Internal/External clients, Legal Department, organizational senior management, and Subject Matter Experts (SMEs) to:
    1. Create and maintain a strategic and comprehension security program
    2. Ensure alignment between security and privacy compliance programs including policies, practices and investigations
    3. Establish governance for the corporate-wide security program, including physical and electronic assets
    4. Identify business requirements and implement people, process, technology, and/or oversight/governance to achieve desired outcome(s)
v. Communicate well AND to effectively champion for important security concern protections
vi. Create a culture of cyber security both with the IT organization and driving behavioral changes for the business
vii. Initiates and promotes activities to foster information security awareness within the organization and related entities
viii. Possess information security consultant skills to support department interaction to properly identify all data security related issues and needs
ix. Present at security industry events

e. ***PROCESS***
   i. Ability to assess third party security requirements
   ii. Address disaster recovery, business continuity, risk management and access controls needs of the company
   iii. Manage breach determination and notification processes under privacy laws and applicable State breach rules and requirements
   iv. Establishing and administer processes for security breaches
   v. Develop and implement a security risk management plan
   vi. Develop and managing organizational budgets
   vii. Maintain information security policies, standards, and procedures
   viii. Manage the development and implementation of the global security policy, standards, guidelines and procedures
   ix. Monitor compliance of all vendor agreements to ensure security concerns, requirements, and responsibilities are addressed

f. ***TECHNOLOGY***
   i. Confirm the information technology and information security support the goals and objectives of the organization.
   ii. Determine and prioritize organizational security risks to design and implement information security controls
   iii. Ensure organizational audit controls monitor activity on electronic systems that contain or use protected personal information
   iv. Evaluate emerging cybersecurity and IT technologies for adoption within the organization, as well as provide guidance to sales and engineering teams
   v. Evaluate new security technology & trends, evolving threats, risks and vulnerabilities and provides recommendations to strengthen internal and external information security environment
   vi. Safeguard physical security of the organization, to include asset protection, workplace violence prevention, access control systems, video surveillance, and alike systems

VII. What **skills** would a **RECENT GRADUATE** need in order to apply for your job? [Check all those that apply]. (**checkbox**)

g. ***PEOPLE***
   i. Act as a liaison to the information systems and compliance departments
   ii. Ability to oversee developing and delivery of initial and ongoing security training to the workforce.
   iii. Application of current compliance and governance issues and corrective measures (regulatory mandates, including PCI DSS, SOC 2 Type II, GDPR, HITRUST, and more.
   iv. Collaborate with the C-suite level managers, Internal/External clients, Legal Department, organizational senior management, and Subject Matter Experts (SMEs) to:
      1. Create and maintain a strategic and comprehension security program
      2. Ensure alignment between security and privacy compliance programs including policies, practices and investigations

3. Establish governance for the corporate-wide security program, including physical and electronic assets
4. Identify business requirements and implement people, process, technology, and/or oversight/governance to achieve desired outcome(s)

v. Communicate well AND to effectively champion for important security concern protections
vi. Create a culture of cyber security both with the IT organization and driving behavioral changes for the business
vii. Initiates and promotes activities to foster information security awareness within the organization and related entities
viii. Possess information security consultant skills to support department interaction to properly identify all data security related issues and needs
ix. Present at security industry events

h. ***PROCESS***
   i. Ability to assess third party security requirements
   ii. Address disaster recovery, business continuity, risk management and access controls needs of the company
   iii. Manage breach determination and notification processes under privacy laws and applicable State breach rules and requirements
   iv. Establishing and administer processes for security breaches
   v. Develop and implement a security risk management plan
   vi. Develop and managing organizational budgets
   vii. Maintain information security policies, standards, and procedures
   viii. Manage the development and implementation of the global security policy, standards, guidelines and procedures
   ix. Monitor compliance of all vendor agreements to ensure security concerns, requirements, and responsibilities are addressed

i. ***TECHNOLOGY***
   i. Confirm the information technology and information security support the goals and objectives of the organization.
   ii. Determine and prioritize organizational security risks to design and implement information security controls
   iii. Ensure organizational audit controls monitor activity on electronic systems that contain or use protected personal information
   iv. Evaluate emerging cybersecurity and IT technologies for adoption within the organization, as well as provide guidance to sales and engineering teams
   v. Evaluate new security technology & trends, evolving threats, risks and vulnerabilities and provides recommendations to strengthen internal and external information security environment
   vi. Safeguard physical security of the organization, to include asset protection, workplace violence prevention, access control systems, video surveillance, and alike systems

VIII. In your opinion, what skills, either for your employment or as needed by a graduate, were missing as witnessed during these ranking exercises? **(open)**

IX. Provided is a general employment listing as seen within general employment ads. Please select those skills you require in order to hire a Chief Information Security Officer: (**checkbox**)
   a. C, C++, C#, Java and/or PHP programming languages
   b. Enterprise architecture
   c. Firewall and intrusion detection/prevention protocols
   d. Knowledge of third-party auditing and cloud risk assessment methodologies
   e. ISO 27002, ITIL and COBIT frameworks
   f. Network security architecture development and definition
   g. PCI, HIPAA, NIST, GLBA and SOX compliance assessments
   h. Practices and methods of IT strategy
   i. Secure coding practices, ethical hacking and threat modeling
   j. Security architecture
   k. Security concepts related to DNS, routing, authentication, VPN, proxy services and DDOS mitigation technologies
   l. TCP/IP, computer networking, routing and switching
   m. Windows, UNIX and Linux operating systems
   n. Other_List

X. Identify those certificates that are either Required (R), Preferred (P), Not Required (NR) for employment based upon the following listing: (**Dropbox**)
   a. CCISO: Certified Chief Information Security Officer
   b. CGEIT: Certified in the Governance of Enterprise IT
   c. CISA: Certified Information Systems Auditor
   d. CISM: Certified Information Security Manager
   e. CISSP: Certified Information Systems Security Professional
   f. CISSP-ISSMP: Information Systems Security Management Professional
   g. GSLC: GIAC Security Leadership
   h. Other_List

XI. Rank the following certificates, from 1 to 7 with 7 being the most important, based upon their importance to corporate employment: (**ranking exercise**)
   a. CCISO: Certified Chief Information Security Officer
   b. CGEIT: Certified in the Governance of Enterprise IT
   c. CISA: Certified Information Systems Auditor
   d. CISM: Certified Information Security Manager
   e. CISSP: Certified Information Systems Security Professional
   f. CISSP-ISSMP: Information Systems Security Management Professional
   g. GSLC: GIAC Security Leadership
   h. Other_List_Rank

XII. Do you have any comments about your program/degree/skill set listing that you would like to share with the researchers? (**open**)

XIII. Do you give your permission for the researchers to contact you to conduct a follow-up interview or for clarification of open-ended statements? (**Y/N**)
   a. If yes, please indicate your contact information Telephone _____ Email:

Appendix C

"C" Suite Survey - Academicians

Survey Instruments

"C" Suite Survey – Academicians

I. Please indicated your current academic position (**dropdown**)
   a. Lecturer
   b. Assistant Professor
   c. Associate Professor
   d. Professor
   e. Adjunct
   f. Other __List

II. Please indicated your highest degree level completed (**dropdown**)
   a. Associates
   b. Bachelors
   c. Masters
   d. EdD
   e. PhD
   f. Terminal Degree __ List
   g. Other __List

III. Does your institution offer (check all that apply): (**checkbox**)
   a. Cyber Security Degree
   b. Information Security and Assurance
   c. Other degrees that support the "C" Suite field (Indicate)

IV. Does your degree implement skills to support the attainment of the following industry certificates [check all that apply]: (**checkbox**)
   a. CISA: Certified Information Systems Auditor
   b. CISM: Certified Information Security Manager
   c. GSLC: GIAC Security Leadership
   d. CCISO: Certified Chief Information Security Officer
   e. CGEIT: Certified in the Governance of Enterprise IT
   f. CISSP: Certified Information Systems Security Professional
   g. CISSP-ISSMP: Information Systems Security Management Professional

V. How do you currently identify job skills to include in your degree program (**open**)

NOTE TO IRB: This ranking survey question will be repeated for each of the "C" Suite Levels (Questions VI – XI.

VI. The following survey areas, Questions VI – XI, identify required "C" Suite employment skills. This listing was derived from common employment job posting boards, such as Salary.com, Monster.com, and Indeed.com (etc.) with the listing being further reduced and compressed by the researchers to remove repetitive and redundant statements. Further each ranked question is divided into three question dimensions: (a) **People**, (b) **Process**, and (c) **Technology**. Each question will examine one "C" Suite Level at a time: **(a) Chief Executive Officer (CEO), Chief Finance Officer (CFO), Chief Information Officer (CIO), Chief Information Security Officer (CISO), Chief Risk Officer (CRO), and Chief Security Officer (CSO).**

This is a ranking exercise. When selecting your rank for each Skills/Knowledge statement, please do so with the proper dimension in mind: **CEO. (Ranking exercise)**

a. ***PEOPLE***: Please rank the following skills by importance (e.g. a CIO is responsible for 1, 2, 3) with 1 being the most important and **X** being the least.
    i. Act as a liaison to the information systems and compliance departments
    ii. Ability to oversee developing and delivery of initial and ongoing security training to the workforce.
    iii. Application of current compliance and governance issues and corrective measures (regulatory mandates, including PCI DSS, SOC 2 Type II, GDPR, HITRUST, and more.
    iv. Collaborate with the C-suite level managers, Internal/External clients, Legal Department, organizational senior management, and Subject Matter Experts (SMEs) to:
        1. Create and maintain a strategic and comprehension security program
        2. Ensure alignment between security and privacy compliance programs including policies, practices and investigations
        3. Establish governance for the corporate-wide security program, including physical and electronic assets
        4. Identify business requirements and implement people, process, technology, and/or oversight/governance to achieve desired outcome(s)
    v. Communicate well AND to effectively champion for important security concern protections
    vi. Create a culture of cyber security both with the IT organization and driving behavioral changes for the business
    vii. Initiates and promotes activities to foster information security awareness within the organization and related entities
    viii. Possess information security consultant skills to support department interaction to properly identify all data security related issues and needs
    ix. Present at security industry events

b. ***PROCESS***: Please rank the following skills by importance (e.g. a CIO is responsible for 1, 2, 3) with 1 being the most important and **X** being the least.
    i. Ability to assess third party security requirements
    ii. Address disaster recovery, business continuity, risk management and access controls needs of the company
    iii. Manage breach determination and notification processes under privacy laws and applicable State breach rules and requirements
    iv. Establishing and administer processes for security breaches
    v. Develop and implement a security risk management plan
    vi. Develop and managing organizational budgets
    vii. Maintain information security policies, standards, and procedures
    viii. Manage the development and implementation of the global security policy, standards, guidelines and procedures
    ix. Monitor compliance of all vendor agreements to ensure security concerns, requirements, and responsibilities are addressed

c. ***TECHNOLOGY***: Please rank the following skills by importance (e.g. a CIO is responsible for 1, 2, 3) with 1 being the most important and **X** being the least.
    i. Confirm the information technology and information security support the goals and objectives of the organization.
    ii. Determine and prioritize organizational security risks to design and implement information security controls
    iii. Ensure organizational audit controls monitor activity on electronic systems that contain or use protected personal information
    iv. Evaluate emerging cybersecurity and IT technologies for adoption within the organization, as well as provide guidance to sales and engineering teams
    v. Evaluate new security technology & trends, evolving threats, risks and vulnerabilities and provides recommendations to strengthen internal and external information security environment
    vi. Safeguard physical security of the organization, to include asset protection, workplace violence prevention, access control systems, video surveillance, and alike systems

VII. The following survey area is divided into three question dimensions: (a) **People**, (b) **Process**, and (c) **Technology**. This is a ranking exercise. When selecting your rank for each Skills/Knowledge statement, please do so with the proper dimension in mind: **CFO**. (**ranking exercise**)
    i. XXX
    ii. XXX, etc.

VIII. The following survey area is divided into three question dimensions: (a) **People**, (b) **Process**, and (c) **Technology**. This is a ranking exercise. When selecting your rank for each Skills/Knowledge statement, please do so with the proper dimension in mind: **CIO**. (**ranking exercise**)
    i. XXX
    ii. XXX, etc.

IX. The following survey area is divided into three question dimensions: (a) **People**, (b) **Process**, and (c) **Technology**. This is a ranking exercise. When selecting your rank for each Skills/Knowledge statement, please do so with the proper dimension in mind: **CISO**. (**ranking exercise**)
    i. XXX
    ii. XXX, etc.

X. The following survey area is divided into three question dimensions: (a) **People**, (b) **Process**, and (c) **Technology**. This is a ranking exercise. When selecting your rank for each Skills/Knowledge statement, please do so with the proper dimension in mind: **CRO**. (**ranking exercise**)
    i. XXX
    ii. XXX, etc.

XI. The following survey area is divided into three question dimensions: (a) **People**, (b) **Process**, and (c) **Technology**. This is a ranking exercise. When selecting your rank for each Skills/Knowledge statement, please do so with the proper dimension in mind: **CSO**. (**ranking exercise**)
    i. XXX

ii. XXX, etc.

XII. Were any of the responsibilities that were mentioned in the previous questions included in your degree objectives listing **(Y/N)**

XIII. If you indicated Yes as your answer to Question XII, please select those as needed: **(checkbox)**

a. ***PEOPLE***
   i. Act as a liaison to the information systems and compliance departments
   ii. Ability to oversee developing and delivery of initial and ongoing security training to the workforce.
   iii. Application of current compliance and governance issues and corrective measures (regulatory mandates, including PCI DSS, SOC 2 Type II, GDPR, HITRUST, and more.
   iv. Collaborate with the C-suite level managers, Internal/External clients, Legal Department, organizational senior management, and Subject Matter Experts (SMEs) to:
      1. Create and maintain a strategic and comprehension security program
      2. Ensure alignment between security and privacy compliance programs including policies, practices and investigations
      3. Establish governance for the corporate-wide security program, including physical and electronic assets
      4. Identify business requirements and implement people, process, technology, and/or oversight/governance to achieve desired outcome(s)
   v. Communicate well AND to effectively champion for important security concern protections
   vi. Create a culture of cyber security both with the IT organization and driving behavioral changes for the business
   vii. Initiates and promotes activities to foster information security awareness within the organization and related entities
   viii. Possess information security consultant skills to support department interaction to properly identify all data security related issues and needs
   ix. Present at security industry events

b. ***PROCESS***
   i. Ability to assess third party security requirements
   ii. Address disaster recovery, business continuity, risk management and access controls needs of the company
   iii. Manage breach determination and notification processes under privacy laws and applicable State breach rules and requirements
   iv. Establishing and administer processes for security breaches
   v. Develop and implement a security risk management plan
   vi. Develop and managing organizational budgets
   vii. Maintain information security policies, standards, and procedures
   viii. Manage the development and implementation of the global security policy, standards, guidelines and procedures

ix. Monitor compliance of all vendor agreements to ensure security concerns, requirements, and responsibilities are addressed

c. ***TECHNOLOGY***

i. Confirm the information technology and information security support the goals and objectives of the organization.

ii. Determine and prioritize organizational security risks to design and implement information security controls

iii. Ensure organizational audit controls monitor activity on electronic systems that contain or use protected personal information

iv. Evaluate emerging cybersecurity and IT technologies for adoption within the organization, as well as provide guidance to sales and engineering teams

v. Evaluate new security technology & trends, evolving threats, risks and vulnerabilities and provides recommendations to strengthen internal and external information security environment

vi. Safeguard physical security of the organization, to include asset protection, workplace violence prevention, access control systems, video surveillance, and alike systems

XIV. Do you have any comments about your program/degree/skill set listing that you would like to share with the researchers? **(open)**

XV. Do you give your permission for the researchers to contact you to conduct a follow-up interview or for clarification of open-ended statements? **(Y/N)**

a. If yes, please indicate your contact information Telephone _____ Email: _____